Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (previously presented) An information-processing apparatus serving as a data-processing means for carrying out predetermined processing OP1 on input data D1 in order to produce a result of said predetermined processing as processed data D2, said information-processing apparatus comprising:

a data transform means for transforming said input data D1 by using disturbance data XI having a constant Hamming weight, to generate transformed data H1, wherein said input data D1 does not have a constant Hamming weight;

a transformed-data-processing means for carrying out said predetermined processing OP1 for said input data D1 or processing different from said predetermined processing OP1 to replace said predetermined processing OP1 on said transformed data H1 in order to generate processed transformed data H2; and

a data inverse-transform means for carrying out inverse-transformation processing OP2 on said processed transformed data H2 by using processed disturbance data XO having a constant Hamming weight, in order to generate said processed data D2 which can also be obtained without transformations as a result of said predetermined processing OP1 carried out on said input data D1.

2. (previously presented) An information-processing apparatus according to claim 1, wherein said processed disturbance data XO is generated by carrying out said predetermined processing OP1 on said disturbance data XI.

3. (previously presented) An information-processing apparatus according to claim 1, wherein each bit of said processed disturbance data XO and said disturbance data XI has a logic value of 0 or 1 at a probability of 50%.

4. (previously presented) An information-processing apparatus according to claim 1, said information-processing apparatus further having a disturbance-data and processed-disturbance-data generation means capable of generating said disturbance data XI having a constant Hamming weight and generating said processed disturbance data XO having a constant Hamming weight by execution of input-data processing defined in advance on said disturbance data XI.

5. (previously presented) An information-processing apparatus according to claim 1, said information-processing apparatus further having:

a disturbance-data storage means for storing a plurality of candidates for said disturbance data XI having uniform Hamming weights; and

a disturbance-data select means for randomly selecting one of said candidates for said disturbance data XI stored in said disturbance-data storage means,

wherein disturbance-data processing is carried out to process said selected candidate for said disturbance data XI in order to generate said processed disturbance data XO.

6. (previously presented) An information-processing apparatus according to claim 1, said information-processing apparatus further having a constant-Hamming-weight-random-number generation means used for generating random numbers with uniform constant Hamming weights and provided with:

a random-number generation means for generating random numbers each having a Hamming weight equal to half the number of bits included in said generated random number;

a bit inversion means for inverting bits of data; and

a bit concatenation means for concatenating a random number generated by said random-number generation means with data output by said bit inversion means as a result of inversion of said random number generated by said random-number generation means.

7. (previously presented) An information-processing apparatus according to claim 1, said information-processing apparatus further having:

a random-number generation means for generating a random number to be used as said disturbance data XI;

a Hamming-weight computation means for computing a Hamming weight of a random number generated by said random-number generation means;

a Hamming-weight examination means for examining said Hamming weight computed by said Hamming-weight computation means; and

a constant-Hamming-weight assurance means for requesting said random-number generation means to generate another random number for said Hamming-weight examination means' result of examination indicating an inspected Hamming weight not equal to a target Hamming weight.

8. (previously presented) An information-processing apparatus according to claim 1, said information-processing apparatus further having a constant-Hamming-weight-random-number generation means used for generating random numbers with uniform constant Hamming weights and provided with:

a constant-Hamming-weight and constant-fractional-bit-count random-number generation means used for generating partial random numbers with uniform constant Hamming weights and uniform bit counts each equal to a fraction of the bit count of a final random number to be generated;

a random-number-generation control means for controlling said constant-Hamming-weight and constant-fractional-bit-count random-number generation means to generate partial random numbers till a sum of bit counts of said partial numbers equal to said bit count of said final random number; and

a data concatenation means for concatenating said partial random numbers generated by said constant-Hamming-weight and constant-fractional-bit-count random-number generation means to result in said final random number.

9. - 17. (canceled).

18. (currently amended) An information processing apparatus, comprising:

a processor arranged to carry out processing operations;

a storage arranged to store programs and data; and

a data bus which interconnects the processor and the storage;

wherein the processor is further arranged to concatenate a predetermined number of ~~the m-bit~~ m-bit random numbers randomly into first disturbance data of n bits equal to a multiple of ~~m; and~~ m;

wherein the processor is further arranged to transform input data into first transformed data with the first disturbance data, process the first transformed data with a first operation, generate second transformed data, process the first disturbance data with the first operation, generate second disturbance data, and inverse-transform the second transformed data into processed data with the second disturbance ~~data~~ data; and

wherein the appearance probabilities of the logic value 0 or 1 at each bit position of the first disturbance data and the second disturbance data are set at 50%.

19. (canceled)

20. (previously presented) An information processing apparatus according to claim 18, wherein the m-bit random numbers are collected in a table.

21. (previously presented) An information processing apparatus according to claim 18, wherein the processor is arranged to transform the input data into the first

transformed data by means of either one of an XOR operation, an addition operation, or a transform operation with the first disturbance data.

22. (previously presented) An information processing apparatus according to claim 18, wherein the first operation is either one of a rotate operation, a shift operation, or a bit permutation operation.

23. (canceled)

24. (currently amended) An information processing apparatus, comprising:

a processor arranged to carry out processing operations;

a storage arranged to store programs and data; and

a data bus which interconnects the processor and the storage;

wherein the processor is arranged to transform input data into first transformed data with first disturbance data, process the first transformed data with a first operation, generate second transformed data, process the first disturbance data with the first operation, generate second disturbance data, and inverse-transform the second transformed data into processed data with the second disturbance data~~An information processing apparatus according to claim 23~~, and

wherein the appearance probabilities of the logic value 0 or 1 at each bit position of the first disturbance data and the second disturbance data area set at 50%.

25. (currently amended) An information processing apparatus according to ~~claim 23~~ claim 24,

wherein the processor is arranged to transform the input data into the first transformed data by means of either one of an XOR operation, an addition operation, or a transform operation with the first disturbance data.

26. (currently amended) An information processing apparatus according to ~~claim 23~~ claim 24,

wherein the first operation is either one of a rotate operation, a shift operation, or a bit permutation operation.

27. (new) An information-processing apparatus serving as a data-processing means for carrying out predetermined processing OP1 on input data D1 in order to produce a result of said predetermined processing as processed data D2, said information-processing apparatus comprising:

a data transform means for transforming said input data D1 by using disturbance data XI having a constant Hamming weight, to generate transformed data H1;

a transformed-data-processing means for carrying out said predetermined processing OP1 for said input data D1 or processing different from said predetermined processing OP1 to replace said predetermined processing OP1 on said transformed data H1 in order to generate processed transformed data H2; and

a data inverse-transform means for carrying out inverse-transformation processing OP2 on said processed transformed data H2 by using processed

disturbance data XO having a constant Hamming weight, in order to generate said processed data D2 which can also be obtained without transformations as a result of said predetermined processing OP1 carried out on said input data D1.